Análisis de Protocolos de Comunicaciones para Internet de las Cosas

Mg. Jorge Eterovic; Esp. Marcelo Cipriano; Santiago Nicolet

Instituto de Investigación en Ciencia y Tecnología
Dirección de Investigación Vicerrectorado de Investigación y Desarrollo.
Universidad del Salvador.
Lavalle 1854 – C1051AAB -Ciudad Autónoma de Buenos Aires - Argentina

jorge.eterovic@gmail.com; cipriano1.618@gmail.com; santiago.nicolet@usal.edu.ar

RESUMEN

Internet de las cosas (en inglés, Internet of Things, abreviado: IoT) [1,2] es un concepto que se refiere a la interconexión digital de cosas u objetos en Internet [3]. Según la consultora Gartner [4], en 2020 habrá en el mundo aproximadamente 26 mil millones de dispositivos con un sistema de conexión a Internet de las cosas.

Entre las tecnologías de comunicaciones más usadas en IoT se encuentran: RFID - Radio Frequency Identification, NFC - Near Field Communication y WSN - Wireless Sensor Networks.

Para el usuario de IoT, estas tecnologías resultan ser "transparentes". Es decir que se ignora su existencia o se tiene una visión parcial o incompleta de las mismas. Esta "transparencia" también incluye a cuáles son los protocolos adecuados para cada tipo de aplicación y las técnicas de protección y seguridad de las comunicaciones y del transporte y almacenamiento de datos confidenciales y/o sensibles, en los sistemas que así lo requieren.

Esta investigación se centrará en encontrar los indicadores que permitan identificar la mejor solución de comunicaciones en Internet de las Cosas, y que tenga la capacidad de incorporar soluciones de seguridad, tales como Criptografía Ligera o Liviana [5], para garantizar la privacidad y la protección de los datos personales [6].

Palabras Clave:
Internet de las Cosas, Protocolos de Comunicaciones en IoT, Seguridad en IoT.

CONTEXTO

El Vicerrectorado de Investigación y Desarrollo (VRID), perteneciente a la Universidad del Salvador (USAL), dicta las políticas referidas a la investigación, concibiéndola como un servicio a la comunidad, entendiendo que los nuevos conocimientos son la base de los cambios sociales y productivos. Con el impulso de las propias Unidades Académicas, se han venido desarrollando acciones conducentes a concretar proyectos de investigación uni/multidisciplinarios, asociándolos a la docencia de grado y postgrado y vinculando este accionar, para potenciarlo, con otras instituciones académicas del ámbito nacional e internacional.

La Dirección de Investigación, dependiente del VRID, brinda soporte a las distintas Unidades de Investigación y a sus investigadores para el desarrollo de Proyectos y Programas de Investigación, nacionales e internacionales, como así también, apoyo y orientación de recursos para la investigación.

A ella pertenece el Instituto de Investigación en Ciencia y Tecnología (RR 576/12) en el cual se enmarca este proyecto, con una duración de 2 años (2017-2018).

1. INTRODUCCIÓN.

En 1999, Kevin Ashton, miembro fundador del Laboratorio de Investigación Auto-ID Center del MIT [7], hoy llamado Auto-ID Labs, fue el primero que acuñó y usó el término Internet of things (IoT), donde se realizaban investigaciones en el campo de la identificación por radiofrecuencia (RFID) y tecnologías de sensores.

En IoT cada objeto, ya sea virtual o físico, es transmisible, direccionable y accesible a través de Internet. Cada objeto tiene su propia identificación y tiene la capacidad de detectar, procesar y comunicarse [8].

La naturaleza omnipresente de los objetos en IoT hace que los datos que se recopilan y transmiten para uso público y privado sean muy importantes y se debe garantizar la seguridad de los mismos. La integridad y la confidencialidad de los datos transmitidos, así como la autenticación de los objetos son los aspectos clave de la seguridad y de la privacidad en IoT.

En la Fig. 1 se muestra el Hype Cycle elaborado por la consultora Gartner [9] del estado de las tecnologías emergentes. El Hype Cycle es un gráfico que muestra el estado de madurez de la adopción y de la aplicación de una tecnología. IoT, marcada con una línea roja, se encuentra en la fase ascendente de la curva, conocida como "tecnologías disparadoras de innovación".

La seguridad y la privacidad son un tema extenso que cubre toda la pila de protocolos de comunicaciones. Los principales problemas de seguridad en IoT incluyen Autenticación, Identificación y heterogeneidad del dispositivo. Dado que cada dispositivo tiene su propia identificación, será muy difícil identificar miles de millones de dispositivos.

Autenticar cada dispositivo puede ser un trabajo tedioso. Una de las principales preocupaciones de seguridad es la heterogeneidad de dispositivos, que impide aplicar una única solución de seguridad uniforme en todos los casos.

Cada dispositivo tiene diferentes requerimientos de seguridad. La heterogeneidad del dispositivo también puede causar problemas en otros aspectos.

Fig. 1.

La historia de la seguridad de los dispositivos se inicia con las conocidas "etiquetas antirrobo" que se adhieren a libros, prendas y demás objetos en librerías y shoppings. Luego aparecieron otros objetos, como las llaves "codificadas" de vehículos, los "tags" para abonar peajes y tarjetas para el pago electrónico de pasajes en transporte público (tarjetas Monedero, SUBE, etc.). Pero menos conocidos por su reciente aparición y no tan masiva difusión como son los pasaportes, licencias de conducir, documentos de Identidad y hasta incluso minúsculos chips subcutáneos, entre otros dispositivos y sistemas a implementar.

Obviamente existe una gran diferencia entre la Internet convencional e IoT [10]. Las principales características de IoT son: procesamiento lento, memoria limitada y baja potencia. Las redes de IoT se conocen generalmente como redes con pérdidas y de baja potencia (LLN - Low power and Lossy Networks) dado que son susceptibles a que sufran una gran pérdida de datos.

Las principales tecnologías de comunicaciones utilizada en IoT [11] son:

- RFID: Radio Frequency Identification [12]
- WSN: Wireless Sensor Network [13]
- NFC: Near Field Communication [14]
- WiFi: estándar IEEE 802.11n
- Bluethoot

- 4G: la red de telefonía móvil
- LTE - Long Term Evolution
- ZigBee: estándar IEEE 802.15.4
- IEEE 802.11ah
- Z-Wave
- Sigfox
- LoRaWAN

En general, podemos decir que están siendo utilizadas diferentes tecnologías de comunicaciones, dependiendo de la aplicación y sus requerimientos de alcance, volumen de datos, seguridad, consumo de energía, vida útil de la batería, etc.

Las redes de comunicaciones han ido evolucionando hacia el sector del IoT que, aunque actualmente no compite con el sector de la telefonía móvil a nivel comercial, pero ha despertado el interés y la inversión de numerosas empresas en este sector [15].

2. LÍNEAS DE INVESTIGACIÓN y DESARROLLO.

Se realizará un relevamiento, estudio y análisis exhaustivo de los principales protocolos de comunicaciones que podrían ser usados en IoT.

Se analizarán los protocolos para determinar el grado de exposición en los aspectos de privacidad, protección de datos personales y seguridad en las comunicaciones.

Se definirán indicadores para evaluar comportamientos y permitir comparaciones utilizando las experiencias publicadas en trabajos internacionales.

Se volcarán los resultados obtenidos en una tabla comparativa y en gráficos de usabilidad de los protocolos estudiados.

Finalmente se redactará un informe final con los resultados obtenidos.

3. RESULTADOS OBTENIDOS / ESPERADOS.

El objetivo de este proyecto es realizar un análisis comparativo de los protocolos de comunicaciones, de acuerdo con, por ejemplo, indicadores de alcance, velocidad de transmisión de los datos y consumo de energía, para darle seguridad usando Criptografía Ligera o Liviana.

El uso de estos indicadores nos permitirá evaluar comportamientos y permitir comparaciones a fin de poder seleccionar el mejor protocolo de comunicaciones según las necesidades del usuario.

Así se espera que se puede determinar de manera rápida que protocolo de comunicaciones sería recomendable para transmitir una dada cantidad de datos a una determinada velocidad y a una cierta distancia.

También se identificará el nivel de adopción de los distintos protocolos. Tendremos así la posibilidad de establecer cuáles ya ha sido adoptados por la industria, los nuevos estándares publicados en las normas, pero aún no implementados y los desarrollos de próxima evaluación.

Finalmente se redactará un informe final y se presentarán los resultados obtenidos de esta investigación en diferentes congresos, para su difusión y como un aporte al conocimiento de la comunidad científica.

4. FORMACIÓN DE RECURSOS HUMANOS.

El equipo de investigadores pertenece al cuerpo docente de Tecnologías Aplicadas en la Facultad de Ingeniería, el área de la Seguridad Informática, de la Universidad del Salvador.

A fines del año 2017 se han incorporado el Ing. Santiago Nicolet, docente de las carreras de Ingeniería en Informática y de la Licenciatura en Sistemas de Información y el alumno Damián Rodríguez, como colaboradores en el equipo de investigación. Se espera que en breve se incorporen más alumnos.

5. BIBLIOGRAFÍA.

[1] Internet of Things. http://www.cisco.com /web/solutions/trends/iot/overview.html. Ultima vez consultada: febrero de 2018.
[2] Internet de las cosas Cómo la próxima evolución de Internet lo cambia todo http://www.cisco.com/web/LA/soluciones/executive/assets/pdf/internet-of-things-iot-ibsg.pdf. Ultima vez consultada: febrero de 2018.
[3] Conner, Margery; Sensors empower the "Internet of Things"; Issue 10; pp. 32-38. Mayo de 2010; ISSN 0012-7515
[4] Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020. https://www.gartner.com/newsroom /id/ 2636073. Ultima vez consultada: febrero de 2018.
[5] ISO/IEC 29192. Information technogy - Security techniques - Lightweight Cryptography. 2012. https://www.iso.org.
[6] Román R., Nájera P., López J. "Los Desafíos De Seguridad En La Internet De Los Objetos" University of Malaga, España. 2010.
[7] Kevin Ashton; That 'Internet of Things' Thing; http://www.rfidjournal.com/articles /view?4986. Ultima vez consultada: febrero de 2018.
[8] Advancing the IoT for Global Commerce https://autoidlabs.org/. Ultima vez consultada: febrero de 2018.
[9] Gartner's Hype Cycle Special Report for 2017, Gartner Inc. https://www.gartner.com/ smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/. Ultima vez consultada: febrero de 2018.
[10] Differences between the IoT and Traditional Internet by Dr. Opher https://www.rtinsights.com/differences-between-theiot-and-traditional-internet/ Ultima vez consultada: febrero de 2018.
[11] Laeeq, Kashif, and Jawwad A. Shamsi, "A Study of Security Issues, Vulnerabilities and Challenges in Internet of Things," Securing Cyber-Physical Systems, p. 221, 2015.
[12] Radio frequency identification ready to deliver Armed forces communications and electronics association 2005.
http: //www.afcea.org
[13] http://www.lanacion.com.ar/1892969-club-tigre-chips-bajo-la-piel-una-tecnologia-de-identificacion-practica-o-invasiva. Ultima vez consultada: febrero de 2018.
[14] Masanobu Katagi; Shiho Moriai, Lightweight Cryptography for the Internet of Things; Sony Corporation; 2016.
[15] Tecnologías de Comunicaciones para IoT. Link: https://www.efor.es/servicios/ internet-de-las-cosas-iot.html. Ultima vez consultada: febrero de 2018.